The World Internet Security Company

WISekey Managed PKI End-user Manual

Date: January 2011
Version: 1.0.0
Authors: WISeKey SA

WISeKey S.A - World Trade Center II - 29, route de Pré-Bois CP 885 1215 Geneva, Switzerland
Tel: +41 22 594 30 00 - Fax: +41 22 594 30 01
Email: info@wisekey.com - www.wisekey.com

TABLE OF CONTENTS

1 About this document 3
Copyright 3
2 Getting Started 4
3 User Login 4
4 Change Password 5
5 Update User-Profile 5
6 Certificate Enrollment Process 7
7 Renew your certificate 9
8 Certificate Installation 9
8.1 Using Microsoft Internet Explorer 11
8.2 Using Firefox 13
8.3 Using Google Chrome 15
8.4 Using Apple Safari 18
9 Smartcard Certificate Enrollment 19
9.1 Using Microsoft Internet Explorer 19
9.2 Using Mozilla Firefox 20
10 Certificate Management 23
Appendix A: Microsoft Certificate Management 25
Appendix B: Mozilla Firefox Certificate Manager 28

1 About this document

This document describes the procedures for WISeKey managed PKI end-users to manage digital certificates.

Copyright

No part of the contents of this document may be reproduced or distributed in any form or by any means without the prior written permission of WISeKey SA.

is a registered trademark of WISeKey SA.

is a registered trademark of WISeKey SA.

Microsoft, MS are registered trademarks, and Windows is a trademark of Microsoft Corporation.

Published in Geneva, Switzerland, by WISeKey SA.

Copyright © 2008 WISeKey SA.

All Rights Reserved.

2 Getting Started

WISeKey provides a web-based application for end users to manage certificates via URL below:

https://secure.certifyid.com/certifyid/ura/user

Your administrator will create an account for you to logon the application, in which you can:

- Enroll for a certificate;
- Install a certificate;
- Manage certificates;
- Update your profile;
- Change your password.

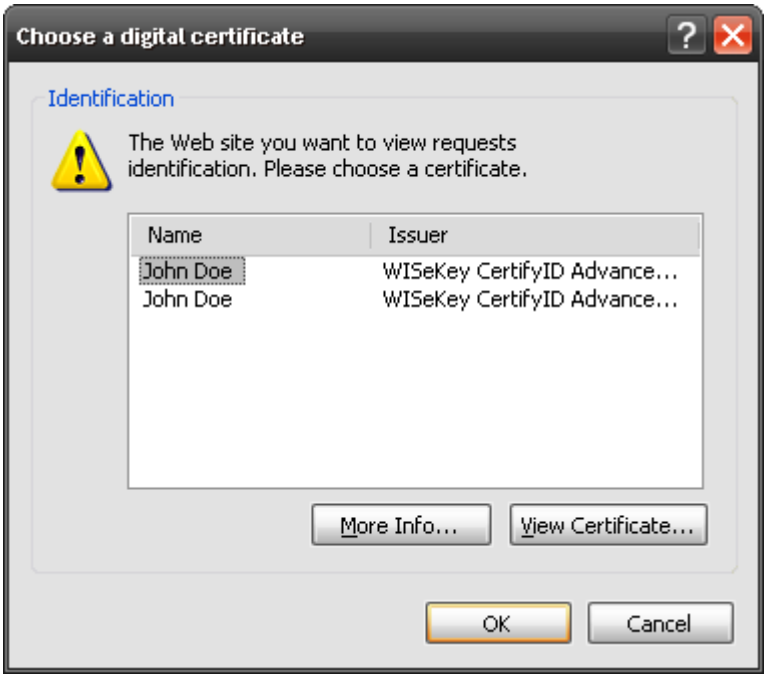
3 User Login

The application provides two options for user authentication including:

- Log into the application by your username and password.
- Log into the application by a digital certificate. This option can be used only after you successfully obtain a certificate.

The picture describes how to log into the application:

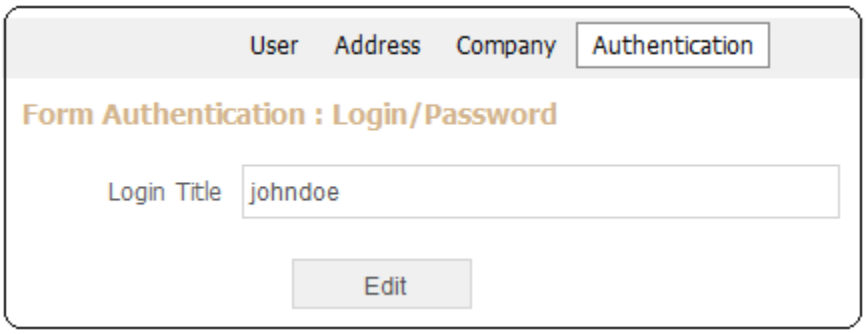
You can click on "**Certificate Logon**" to log into the application by a digital certificate. A window with a list of your digital certificates will be shown for you to choose as follows:



4 Change Password

You can change your password as follows:

- Open "**My Profile**" menu;
- Choose "**Authentication**" tab;
- Choose "**Edit**" button;
- Enter your new password and then click on "**Save"**

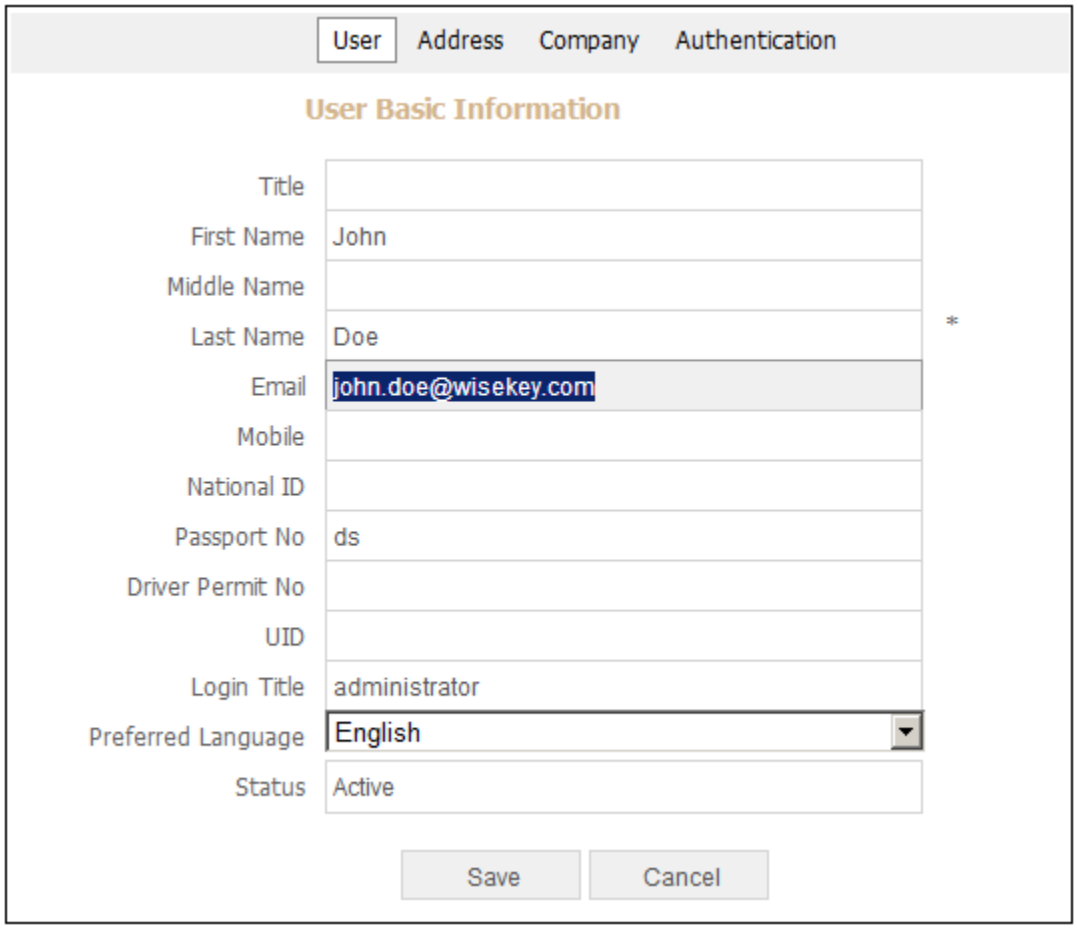


5 Update User-Profile

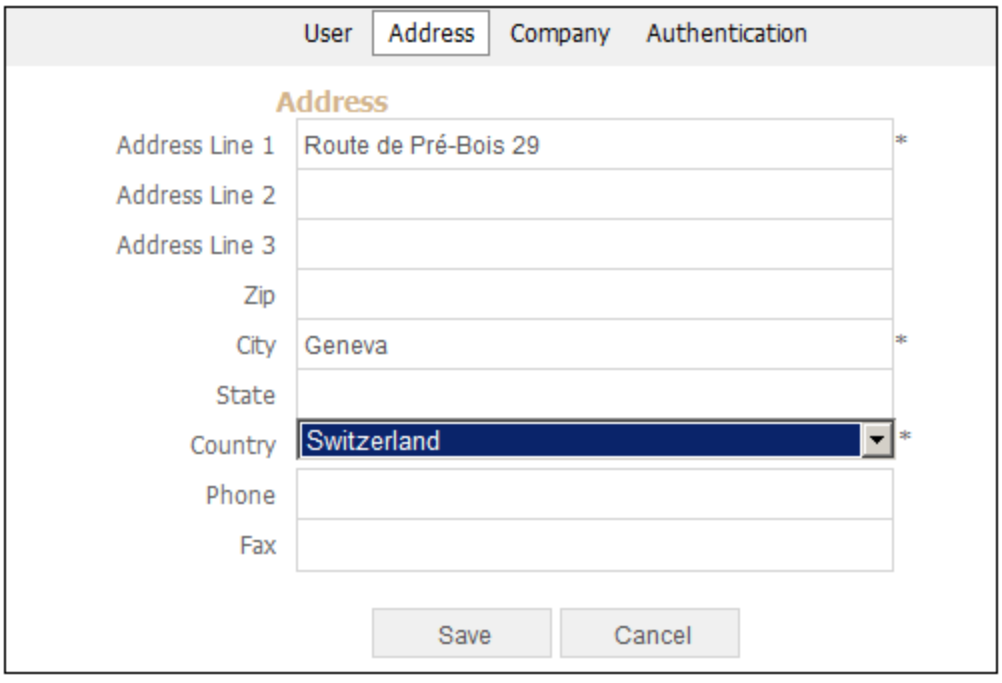
You can update your profile information including:

- Personal information – **User** tab;
- Address – **Address** tab;
- Job title – **Company** tab;

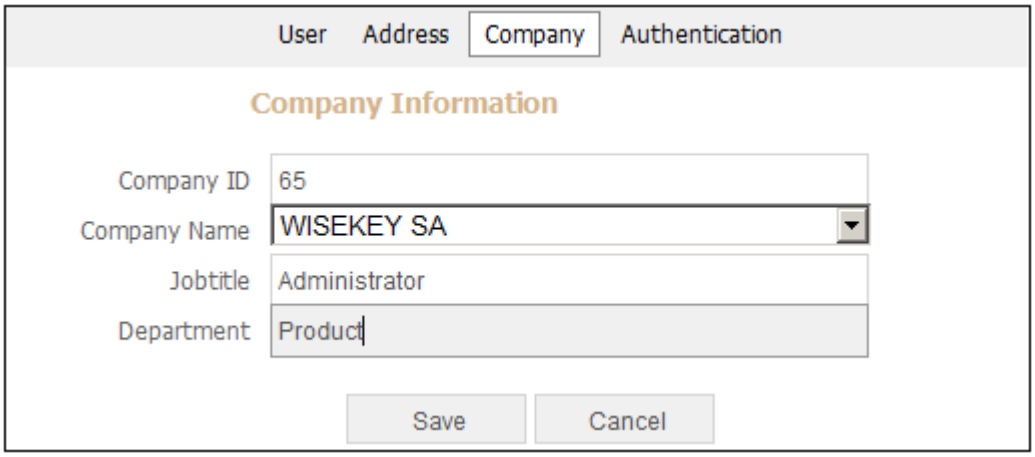
The User tab's interface to update personal information appears as shown below:



Address information can be updated as follows:



Job title and company information can be updated as follows:



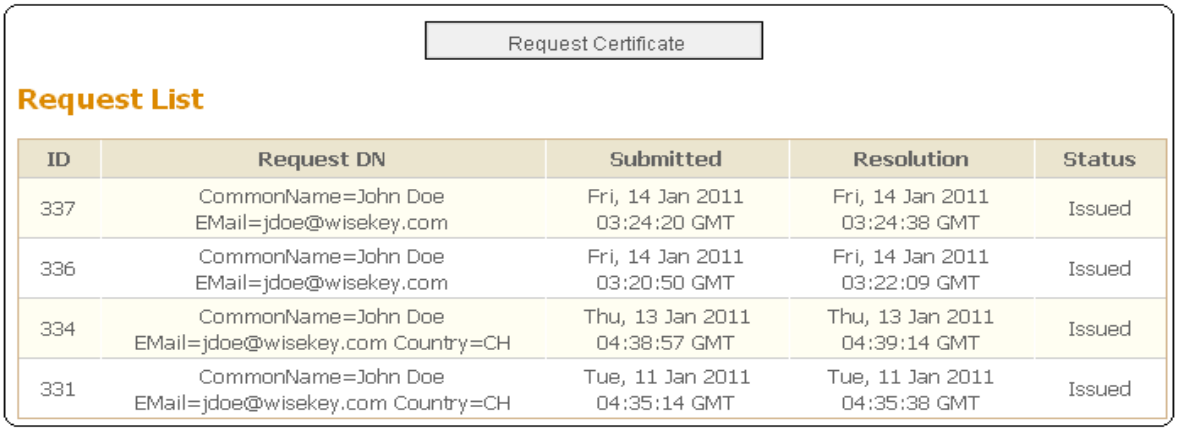
6 Certificate Enrollment Process

To obtain a digital certificate, you need to generate a certificate signing request (CSR) and then submit it to the WISeKey via an online certificate registration form. There are two types of forms for you based on the system configuration:

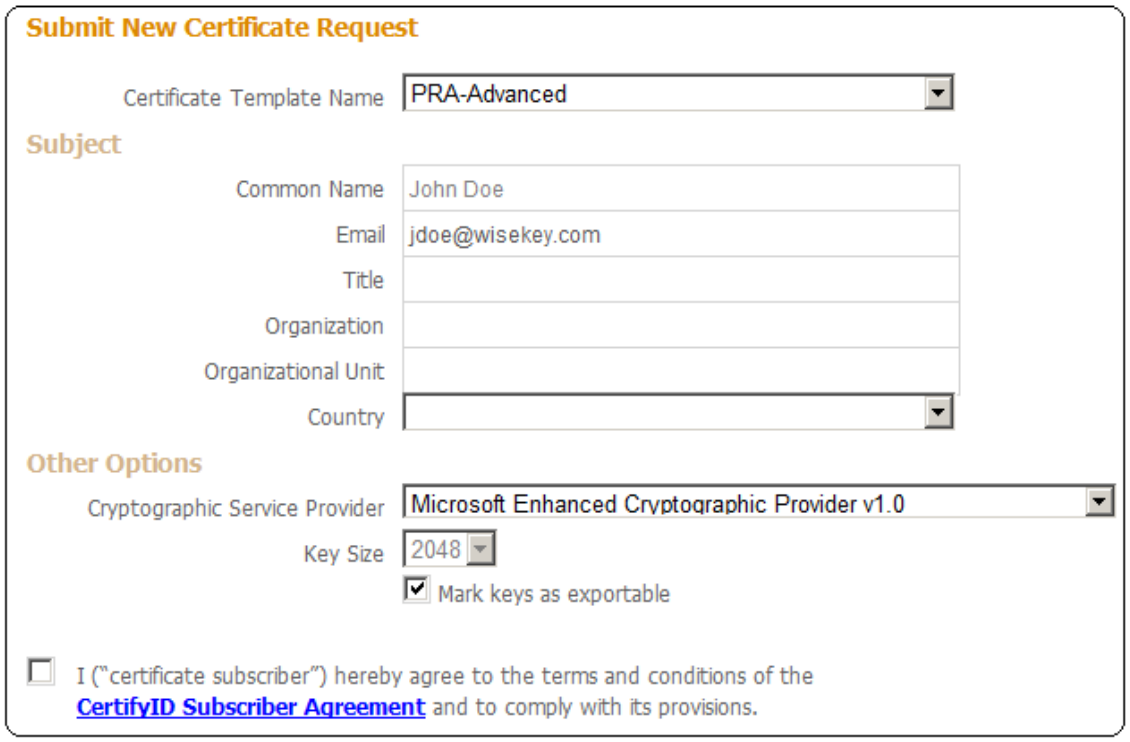
- **Online-form**: You enter subject distinguished names, and/or subject alternative names, and then submit your information. The browser will automatically generate the certificate signing request for you.
- **Offline-form**: You use your existing certificate signing request, edit subject distinguished names, and/or subject alternative names loaded from the request, and then submit the request.

Follow the steps below to submit your certificate signing request

- Choose **"Request"** menu, and then click "**Request Certificate**" button



- The certificate enrollment page should look like below for Microsoft Internet Explorer (IE)



- Below is the certificate enrollment page for non-IE browsers:

- As you see above:
  - **For IE**, you need to follow the steps:
    - Choose a Cryptographic Service Provider (CSP);

- Key length is often fixed;
- Determine if the private key is exportable or not;

▪ **For Non-IE browsers**, choose High-Grade key-size

▪ **For Google Chrome:** The browser allows to generate the CSR, but it does not support certificate installation. Therefore, do not use the Google Chrome browser.

- Finally, click on “Generate” button.

7 Renew your certificate

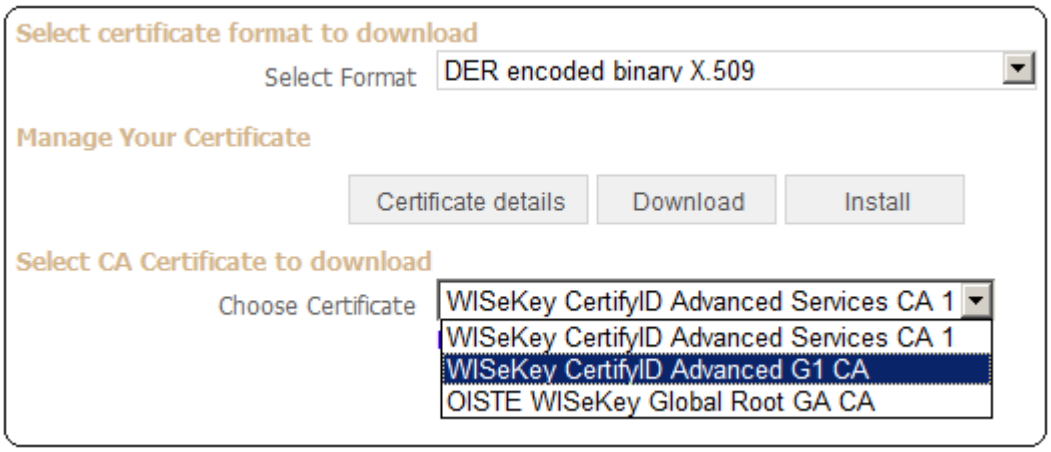
Your certificate can be renewed as follows:

- Choose Certificate menu;
- View the details of the certificate for renewal;
- Click on the Renew button;

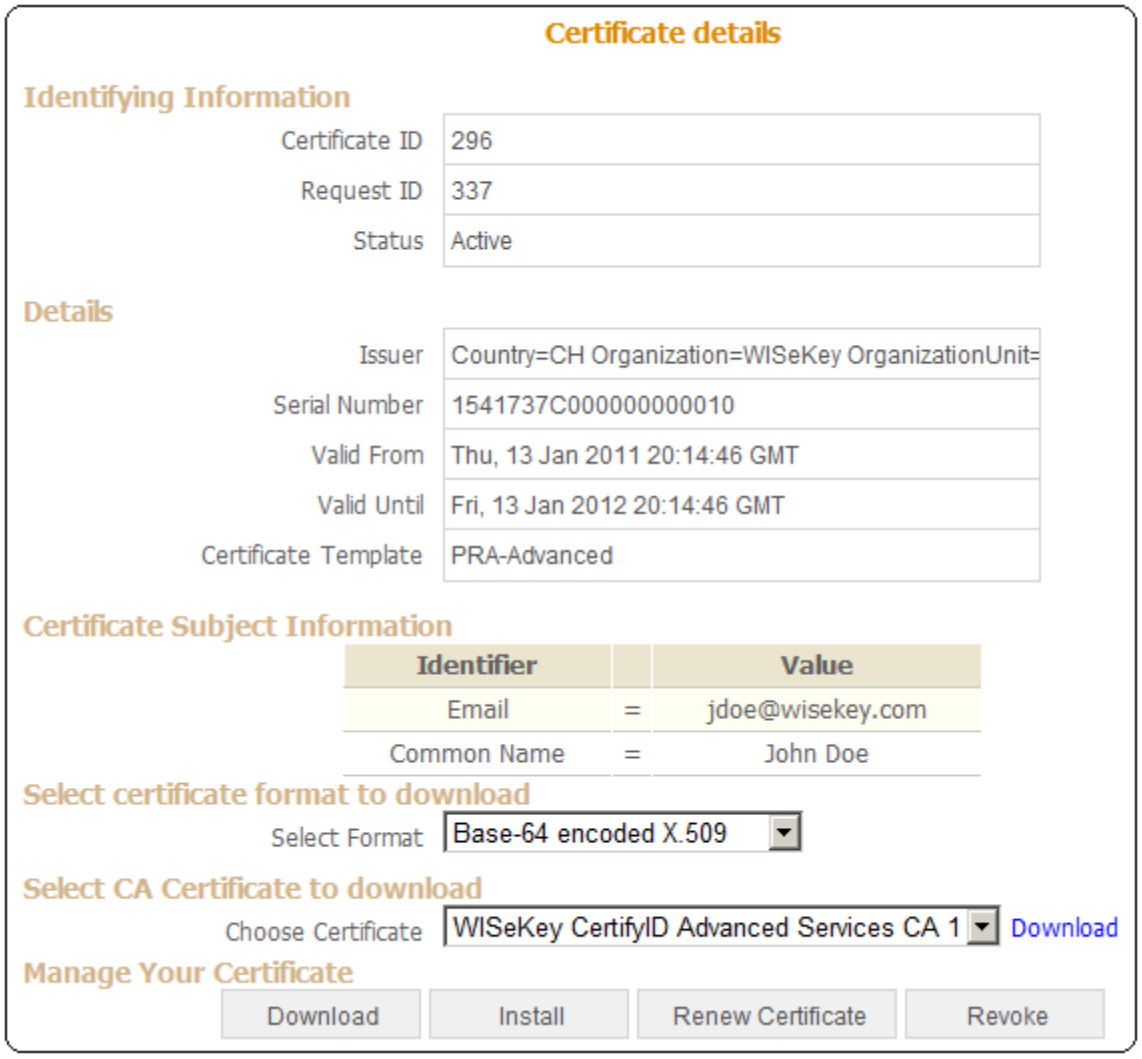
8 Certificate Installation

Your certificate will be issued after the submission of the certificate signing request (CSR). Some certificates are issued immediately, and others require approval by an administrator. You should be notified by email when your certificate is ready. You can view the details of the certificate, download, or install it directly.

The certificate can be installed from the **Certificate-Install** page if it is issued immediately. The page includes the install button as follows:



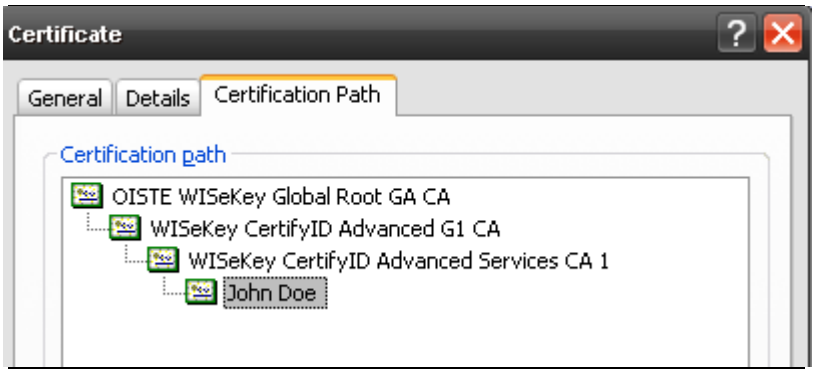
The certificate can be also installed from the **Certificate-View** page if it requires approval by certificate registration officers. Below is a sample view of the page:


Certificate details
Identifying Information
Certificate ID 296
Request ID 337
Status Active
Details
Issuer Country=CH Organization=WISeKey OrganizationUnit=
Serial Number 1541737C000000000010
Valid From Thu, 13 Jan 2011 20:14:46 GMT
Valid Until Fri, 13 Jan 2012 20:14:46 GMT
Certificate Template PRA-Advanced
Certificate Subject Information
Identifier Value
Email = jdoe@wisekey.com
Common Name = John Doe
Select certificate format to download
Select Format Base-64 encoded X.509
Select CA Certificate to download
Choose Certificate WISeKey CertifyID Advanced Services CA 1 Download
Manage Your Certificate
Download Install Renew Certificate Revoke

IMPORTANT:

- The certificate **MUST** be installed from the browser that was used to generate and submit CSR. This means that it is unable to install certificate in Firefox if its CSR was generated by Microsoft Internet Explorer;
- *For Microsoft Windows Users*, each user in a Windows PC has its own user profile and personal certificate store. This means that the user account to install the certificate MUST also be the same user account which generated its CSR; ***these above requirements are also true for a RENEWED certificate.***
- Firefox has its own certificate stores. Therefore, if a certificate is installed in IE, it cannot be used in Firefox, and vice versa.
- If you want to use the certificate in both Firefox and IE, it should be exported from IE, and then imported to Firefox, or vice versa.
- *Please ask your certification authority for further information on the CA certificates that are linked to your certificate*.

Below is a sample entire CA certificate chain that has been correctly installed in Microsoft Windows:



Where:

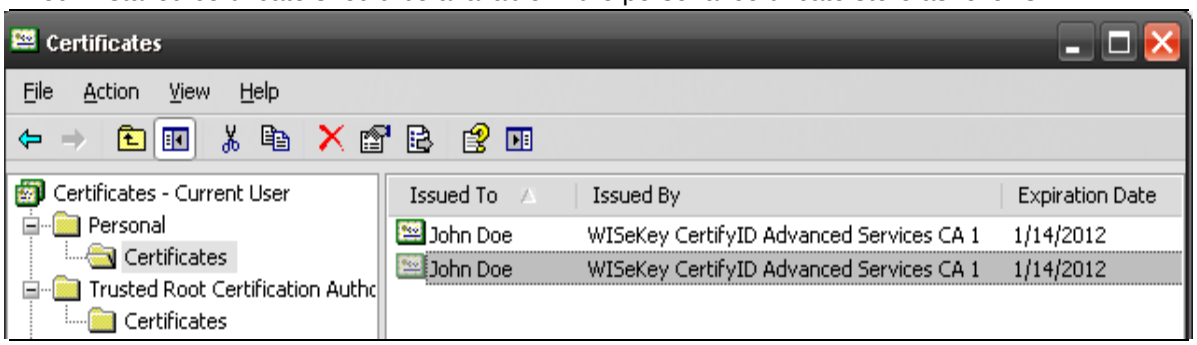
- OISTE WISeKey Global Root GA CA: Root CA Certificate;
- WISeKey CertifyID Advanced G1 CA: Policy CA Certificate;
- WISeKey CertifyID Advanced Services CA 1: Issuing CA Certificate;

8.1 Using Microsoft Internet Explorer

Click **Install** button to install certificate. If the certificate is installed correctly, the following status message will be shown

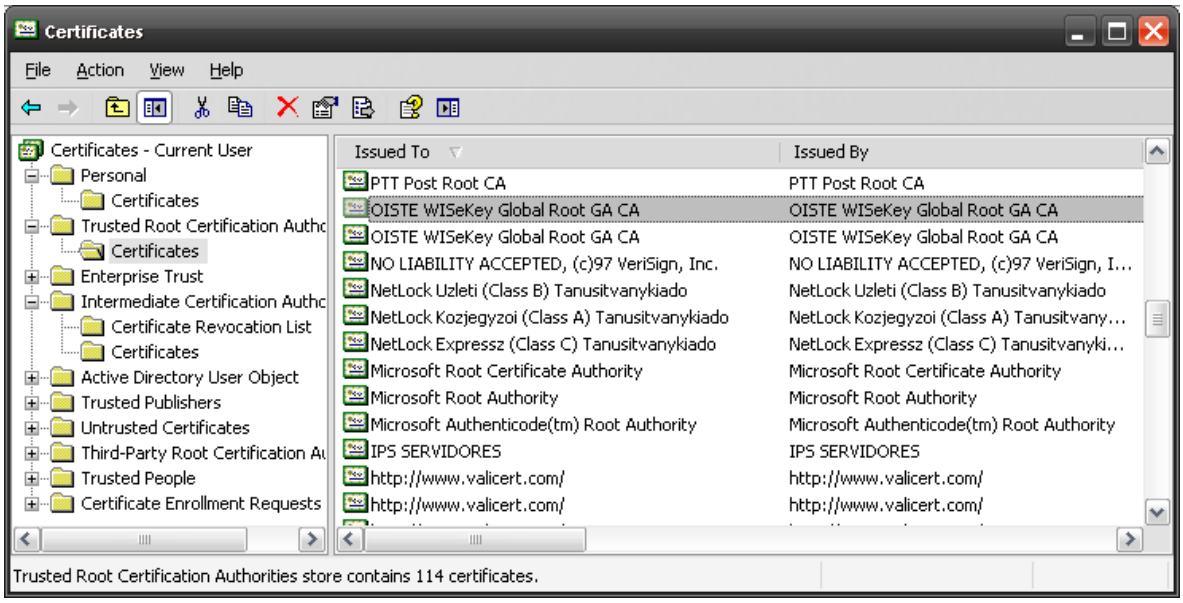
"The Certificate is now installed and ready to be used".

Your installed certificate should be available in the personal certificate store as follows:

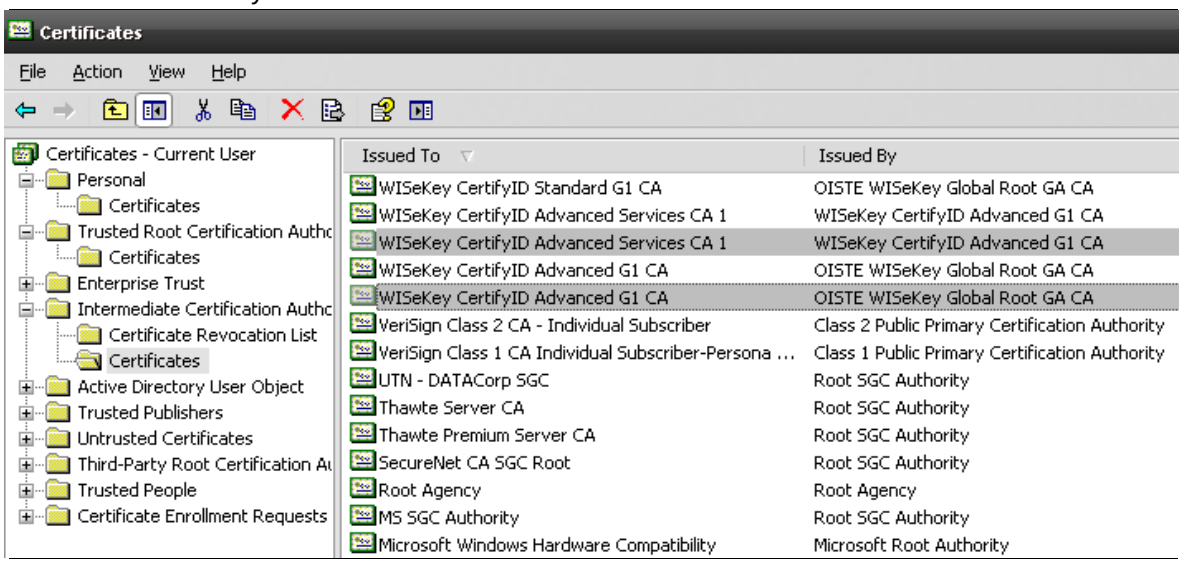


Next, we need to verify the installation of the certificate. Follow the steps below:

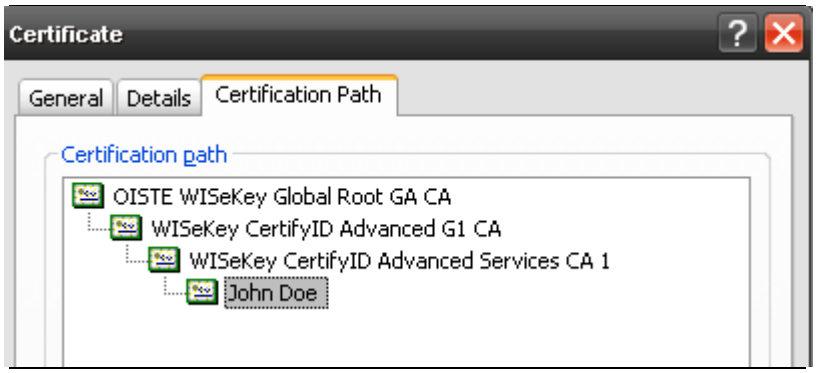
- Open Trusted Root Certification Authorities store, the picture below depicts that the certificate is installed correctly.



- Open Intermediate Certification Authorities Store, the picture below depict that the certificate is installed correctly



- Open Personal Certificate Store, and then open your certificate, if all the certificates were installed correctly, then the certificate view would look like below:



IMPORTANT:

- *Root Certification Authority (CA) Certificate and intermediate CA certificates in the CA certificate chain should be automatically installed in the Windows XP*
- *In Windows 7, the* **OISTE WISeKey Global Root GA CA** *certificate is also installed by the Microsoft Root Certificate Update Program.*
- *Root CA Certificates that are not automatically installed by the Microsoft Root Certificate Update Program must be installed manually.* ***See the Appendix A****.*
- If you get the following error message while installing a certificate in IE8 of Windows 7, Windows Vista, Windows Server 2008 or Windows Server 2008 R2 then please install the hot-fix 2078942 and try re-installing the certificate.
- **ERROR MESSAGE**: *An error occurred when installing your certificate. It might be because that the Root Certificate of your entity certificate was unable to install. Please download the CA chain and follow the instructions in the document below*.

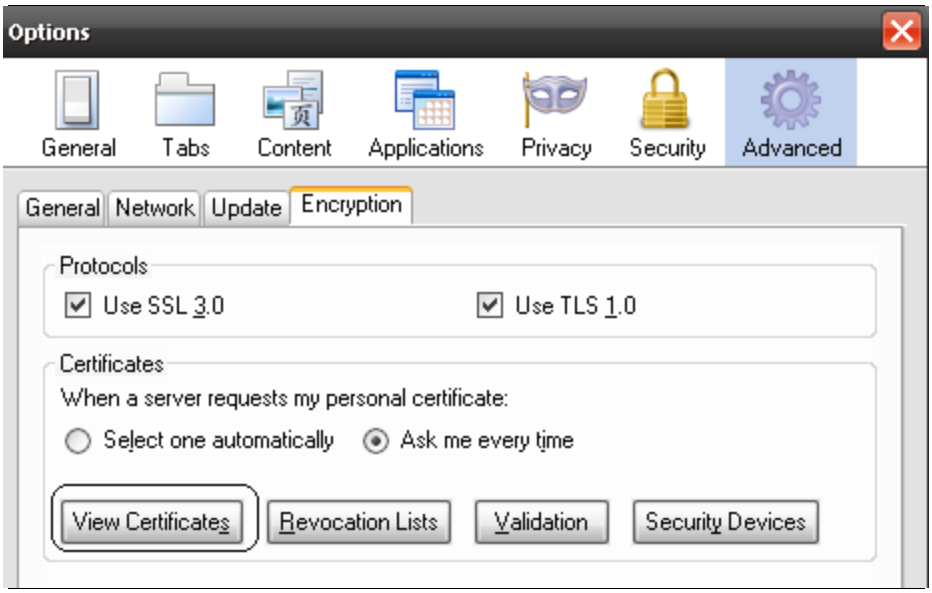
8.2 Using Firefox

Click **Install** button to install certificate. If the certificate is installed correctly, the following status message will be shown

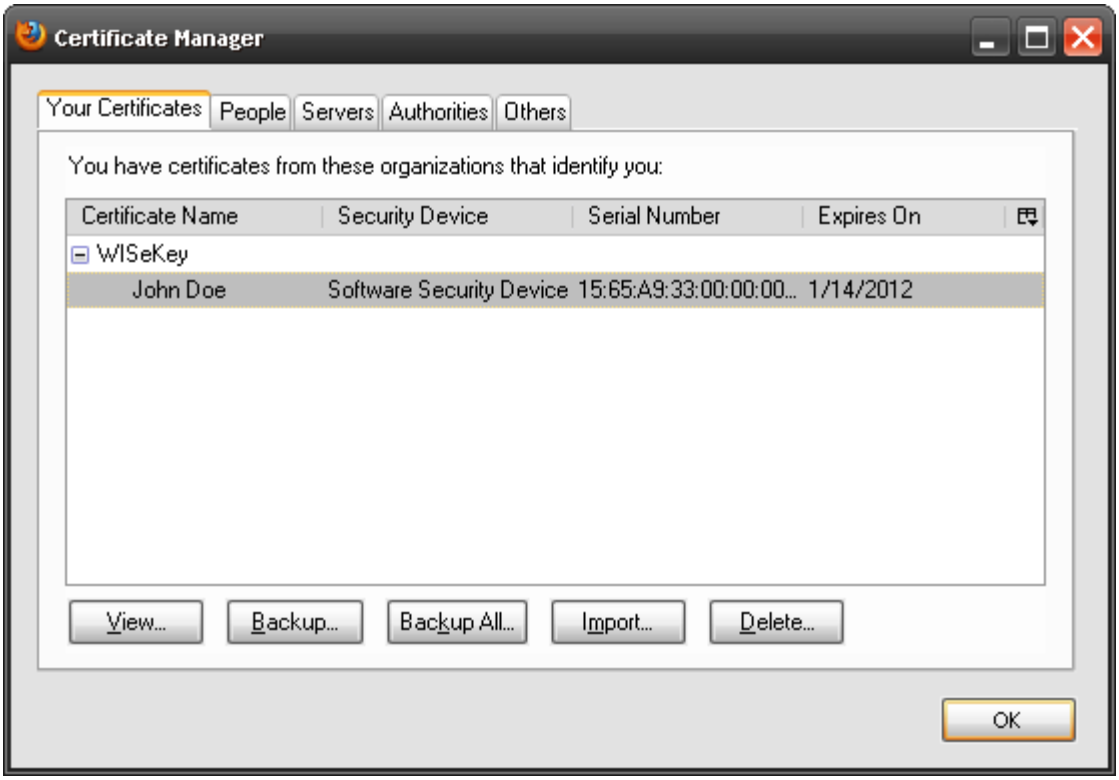
"Your personal certificate has been installed. You should keep a backup of this certificate".

Open Firefox personal certificate store to check if the certificate is installed correctly as follows:

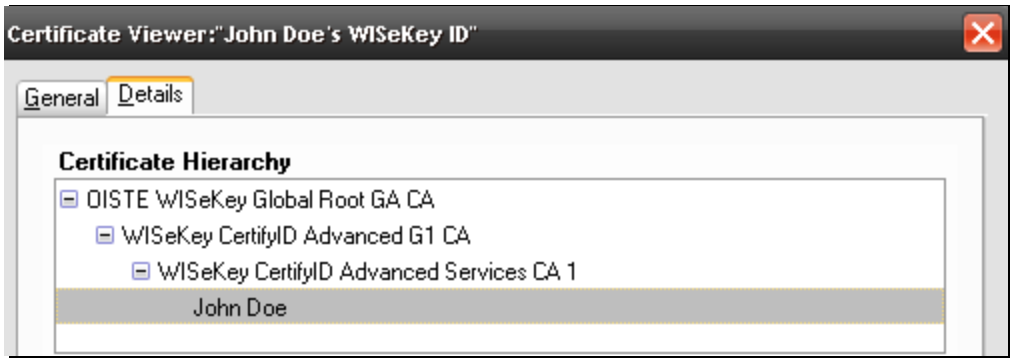
- Open Options window of Firefox, and click "View Certificates"



- Your personal certificates should be listed in the "**Your certificates**" tab



Next, we need to verify the installation of the certificate. If it was installed correctly, then the certification chain of the certificate would look like below:



IMPORTANT:

- *WISeKey CA Certificates are built-in certificates in Firefox, so they should be always available in the certificate store of the browser.*
- *If the built-in certificates are not available, then you can install the certificates manually. See Appendix B.*

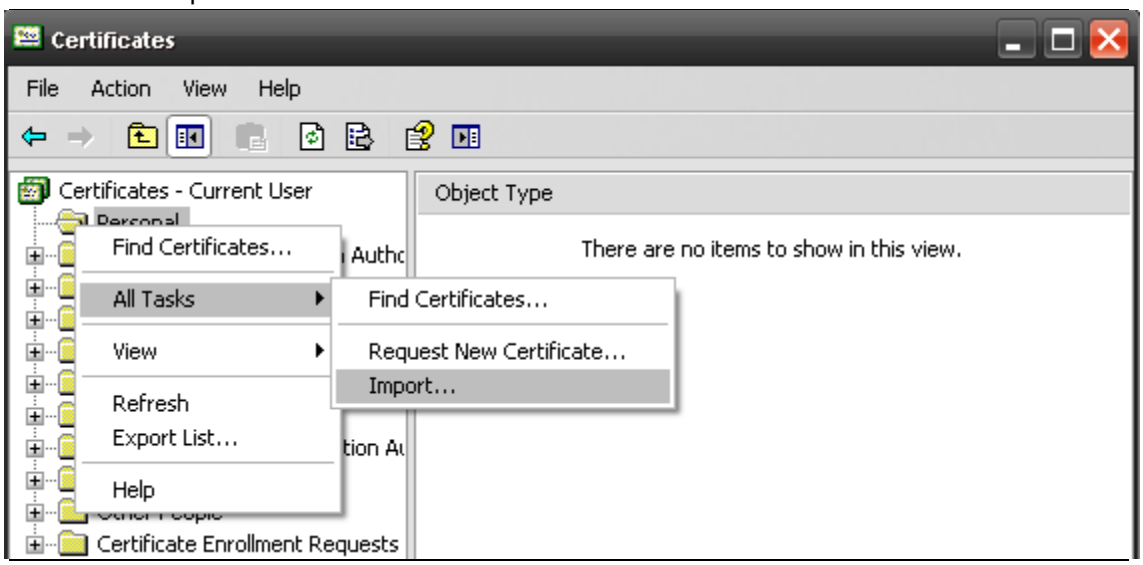
8.3 Using Google Chrome

Like Microsoft Internet Explorer, the browser uses the personal certificate store of the Microsoft Windows, and does not allow installing certificates directly. You have to import the certificate manually:

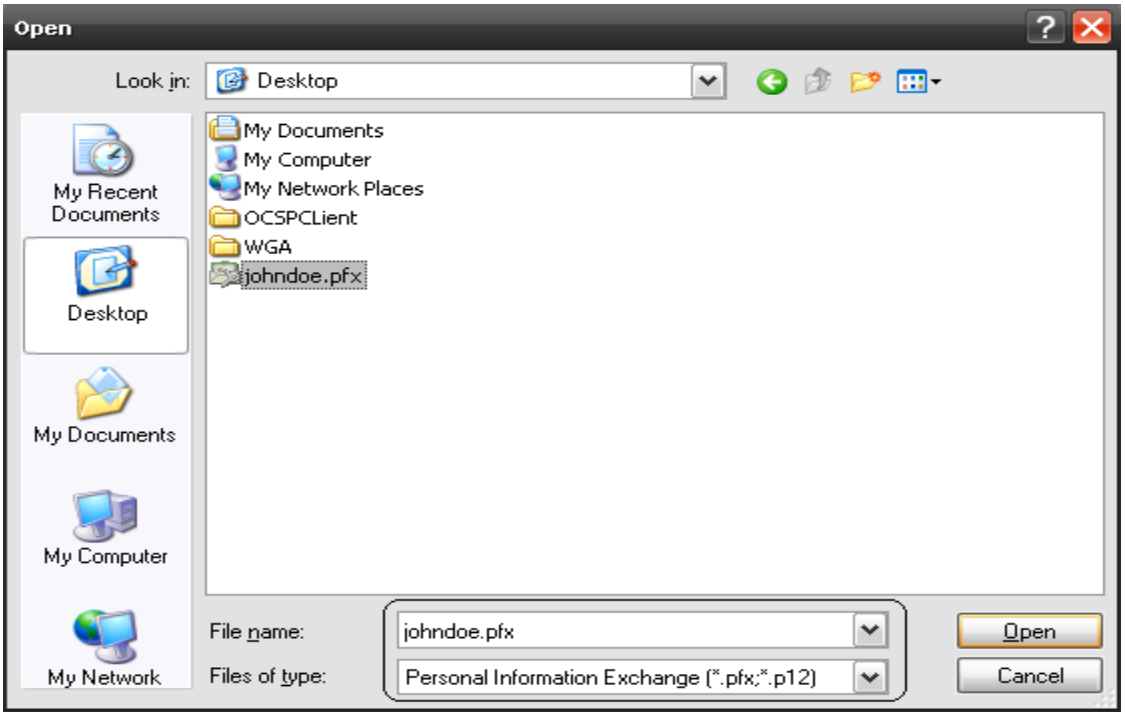
- You can export certificate from Firefox, and then import it to Google Chrome;
- Certificates installed by Microsoft Internet Explorer can be used by Google Chrome.
- Registration Officer can help make a signing certificate request on behalf of you, and you will receive the certificate from the officer.

Follow the steps below to import a certificate; the certificate must be stored in PFX format including a private key:

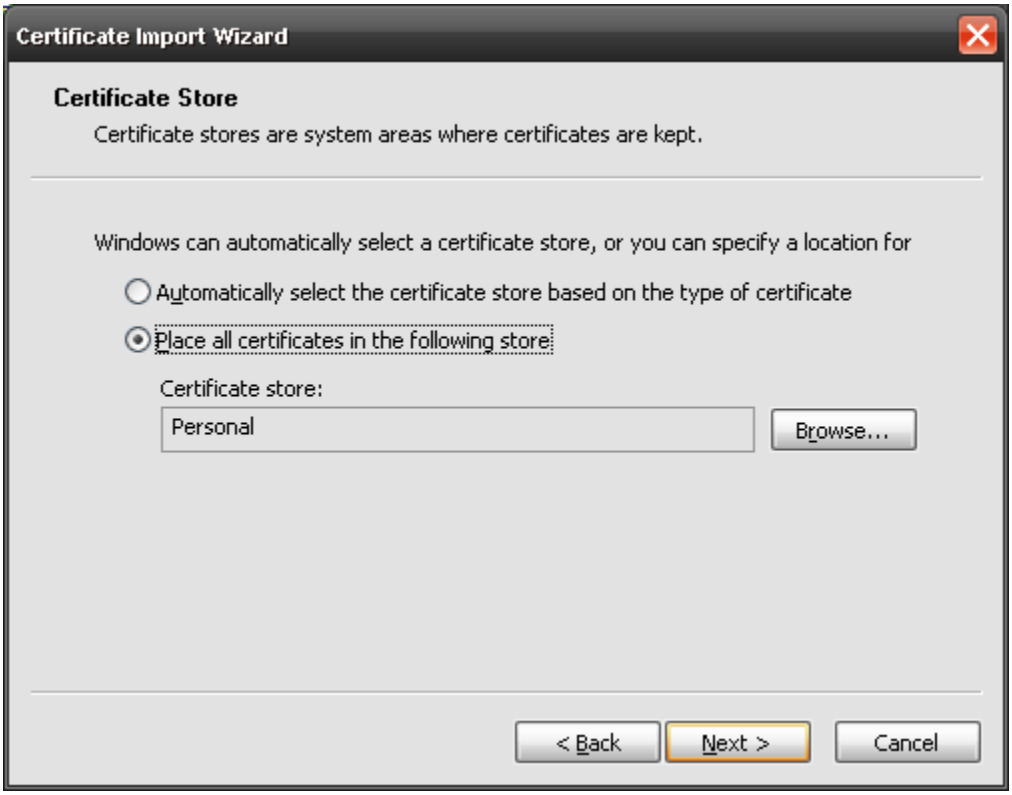
- From **Run** window command, execute "**certmgr.msc**" command, and then choose **Import** menu like the picture below:



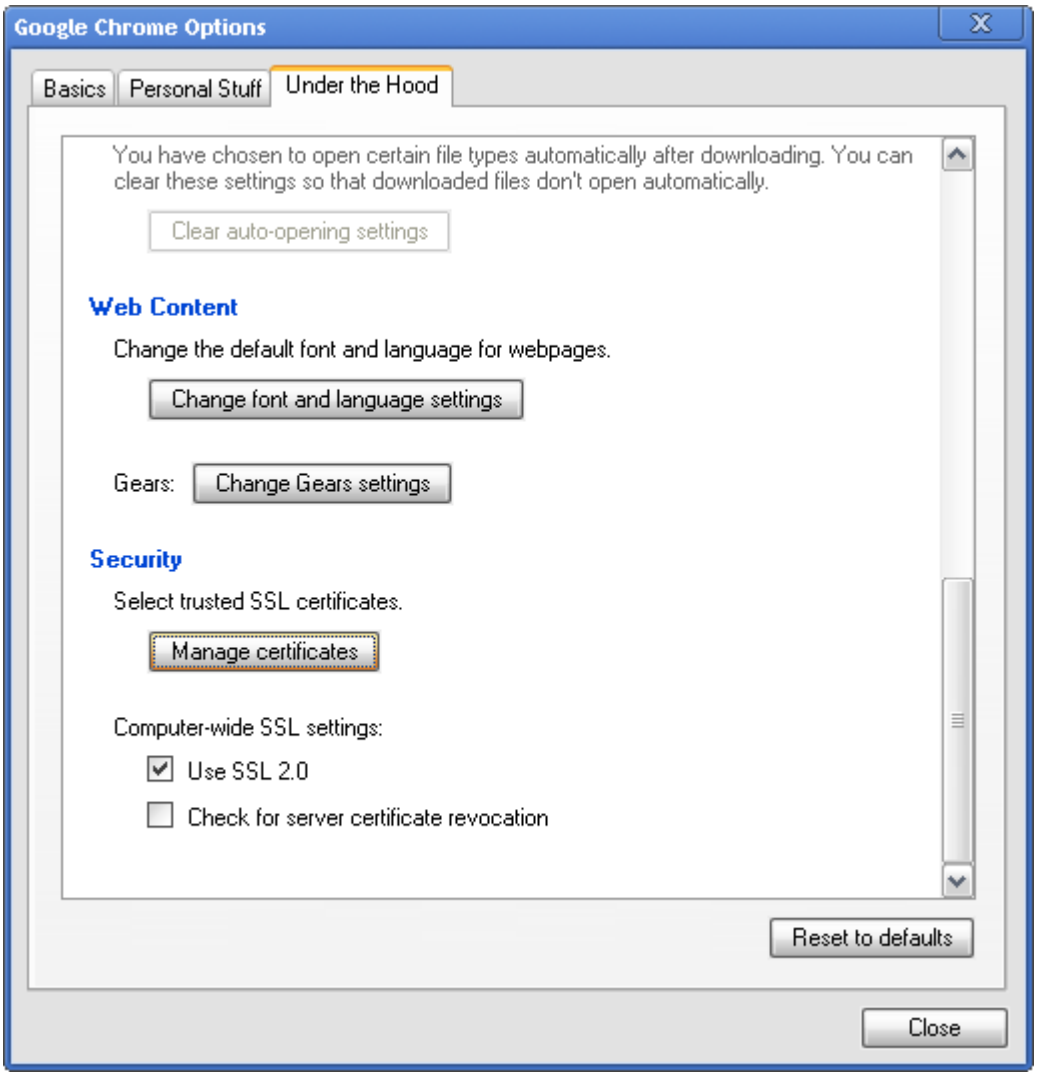
- Choose certificate file to import



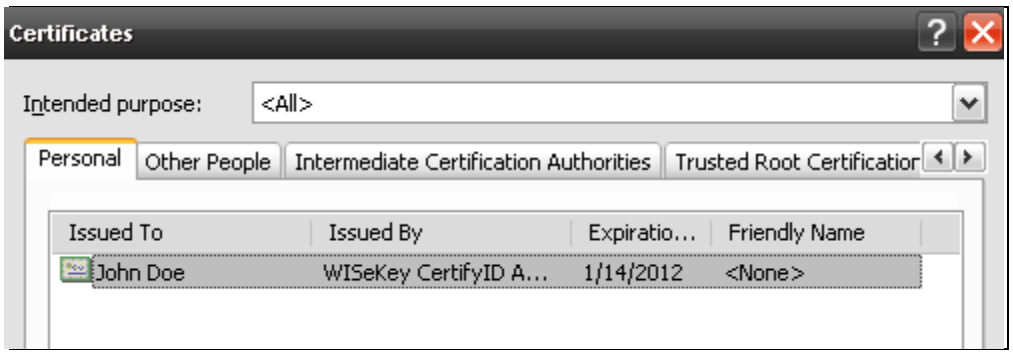
- Enter the password to open the certificate file, and then choose Personal certificate store:


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Personal
Browse...
< Back
Next >
Cancel

- Click Next, and then Finish to complete the wizard.
- Open Google Chrome options, then click “Manage Certificates”


Google Chrome Options
Basics
Personal Stuff
Under the Hood
You have chosen to open certain file types automatically after downloading. You can clear these settings so that downloaded files don't open automatically.
Clear auto-opening settings
Web Content
Change the default font and language for webpages.
Change font and language settings
Gears:
Change Gears settings
Security
Select trusted SSL certificates.
Manage certificates
Computer-wide SSL settings:
Use SSL 2.0
Check for server certificate revocation
Reset to defaults
Close

- Your certificate is now listed in the Personal certificate store.



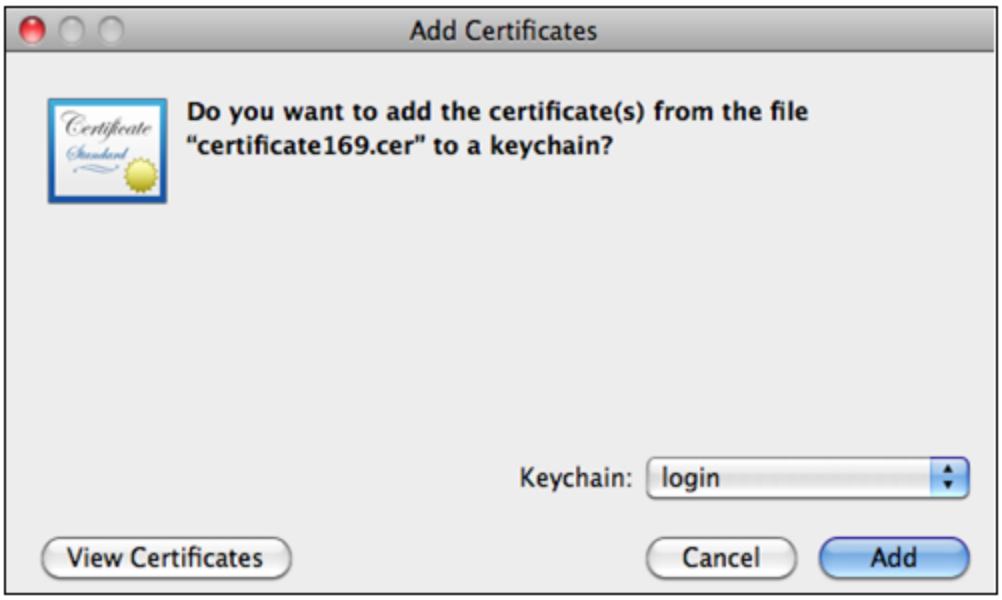
IMPORTANT:

- *You should verify the certificate installation like the section 7.1, because Google Chrome also use system certificate stores as Microsoft Internet Explorer.*

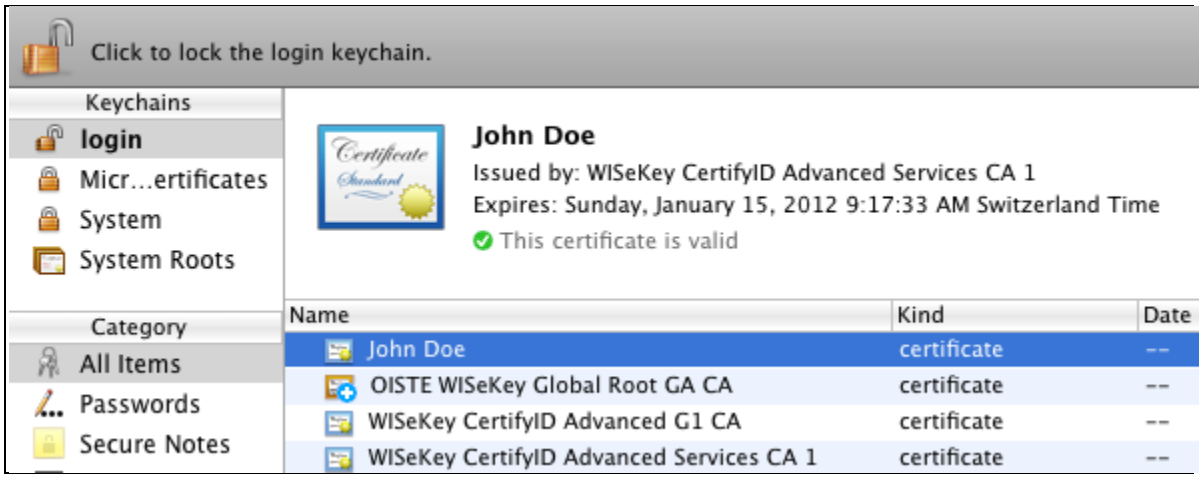
8.4 Using Apple Safari

Follow the steps below to install your digital certificate in Mac OS X 1.6.x:

- In the Certificate Install or Certificate View page, Choose “DER encoded binary X.509”, then download your certificate.
- The Keychain Access program may be opened automatically. If not, you can double click on your certificate file downloaded to open it in the Keychain Access program:



- Click Add button;
- Key Chain might require you to enter your password;
- Now your certificate should be available in the Key Chain list, and with status “This certificate is valid”.



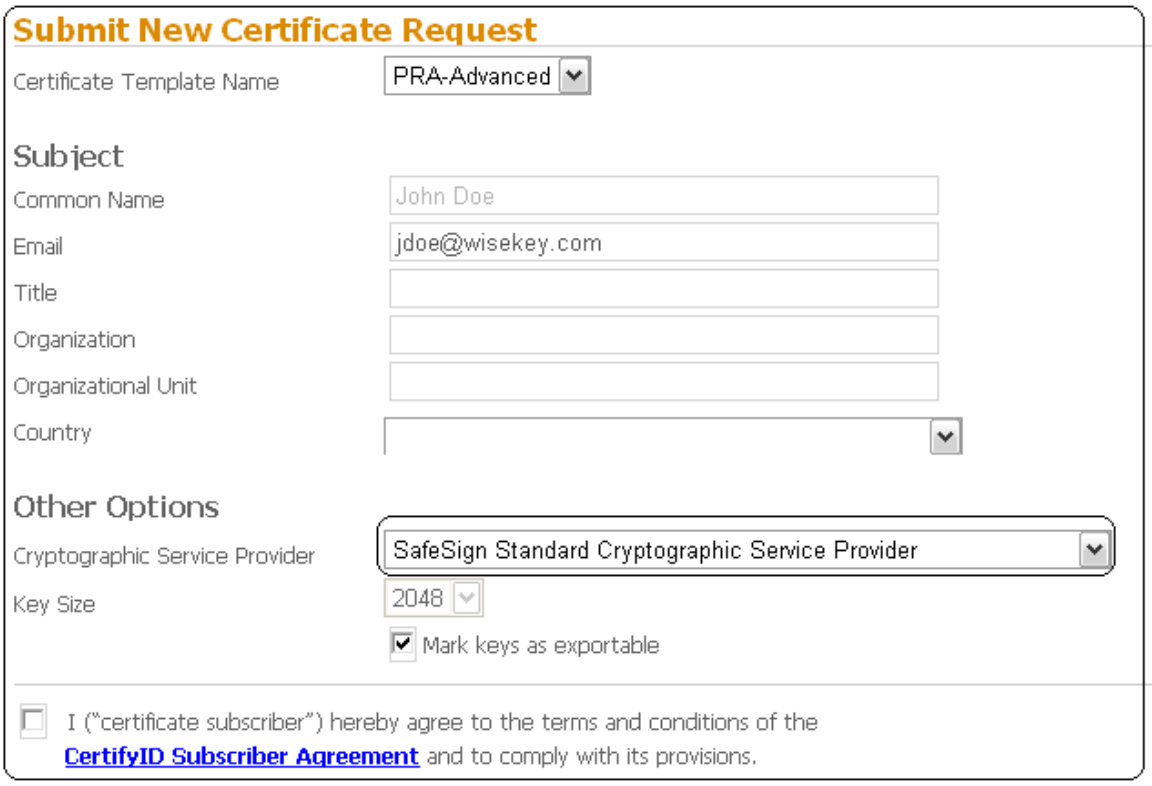
9 Smartcard Certificate Enrollment

The process to obtain a smart card certificate is quite similar to the certificate enrollment process in the section 5. However, there are some differences depending on the browsers.

9.1 Using Microsoft Internet Explorer

Follow the steps below to enroll for a smart card certificate on Microsoft Internet Explorer (IE).

- Choose **"Request"** menu, and then click "**Request Certificate**" button
- The certificate enrollment page should look like below:



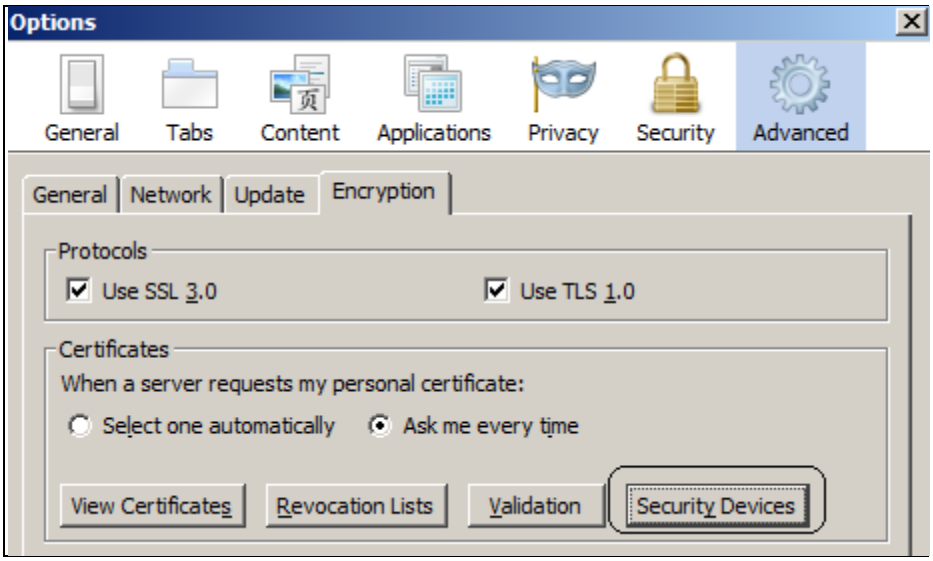
- Below is how the certificate enrollment page looks like on non-IE browsers:

- Choose Cryptographic Service Provider for your Smart card. The picture above uses "SafeSign" Provider.
- Make sure that your smart card has been plugged, and then click on "Generate" button. You then will have to enter PIN. The smart card will take a while to generate the key pair.
- If the certificate is issued immediately, then you click on the Install button in the Certificate Install page.
- If the certificate is issued after approval of your organization registration officer, you must open Microsoft Internet Explorer in the machine you make the request, view detail of the certificate, and then click on Install. See section 9 to know how to browse and view your certificates.

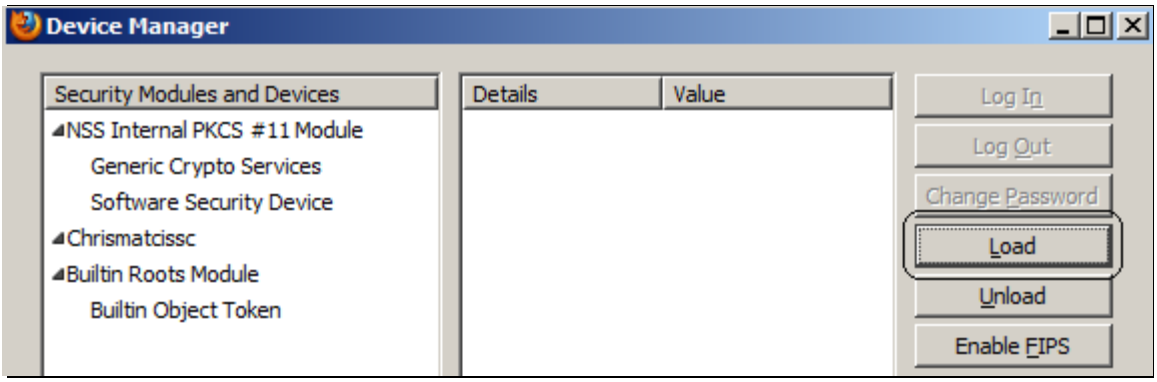
9.2 Using Mozilla Firefox

Mozilla Firefox deals with the smart card directly via the PKCS11 library provided by your smart card provider. In this document, we use Safe-Sign smart card driver.
Follow the steps below:

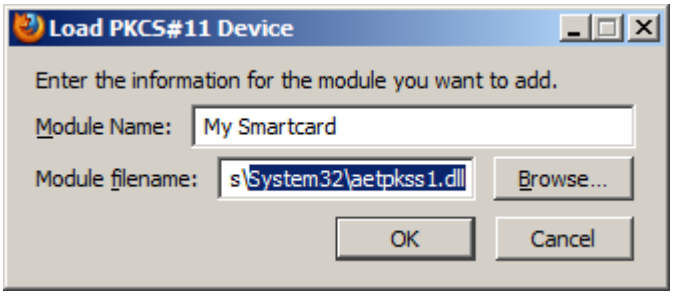
- Open Option window of the browser, choose "Security Devices"



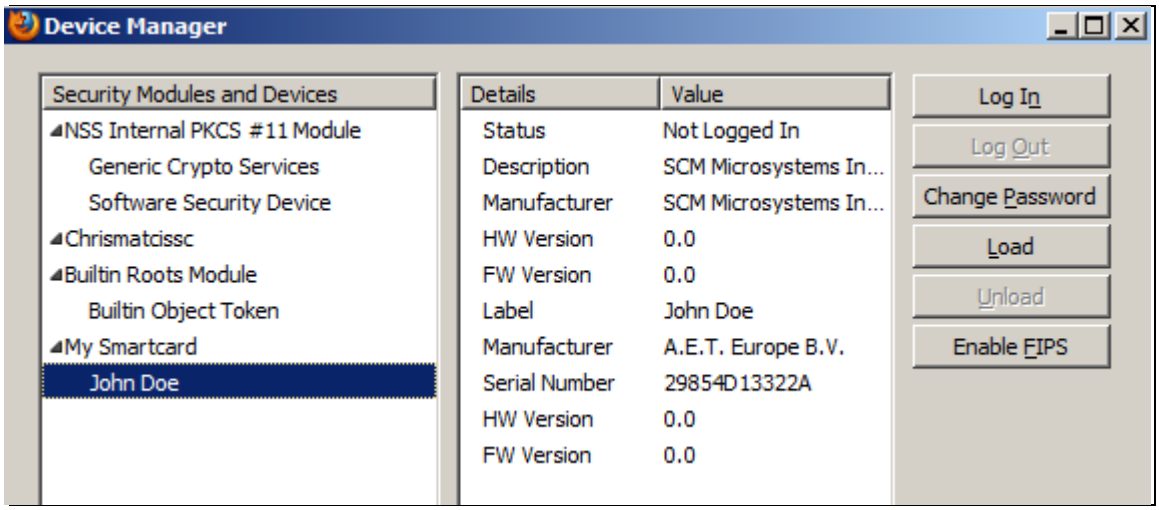
- Then click on Load button:



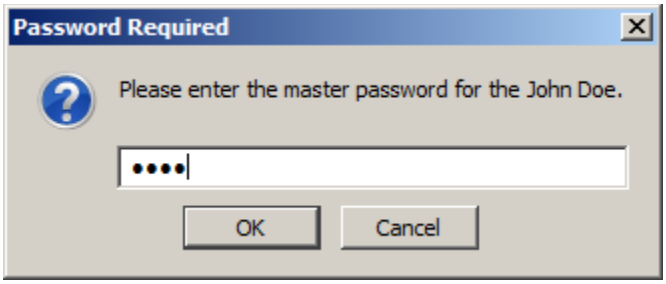
- Browse your PKCS11 driver, and click OK.



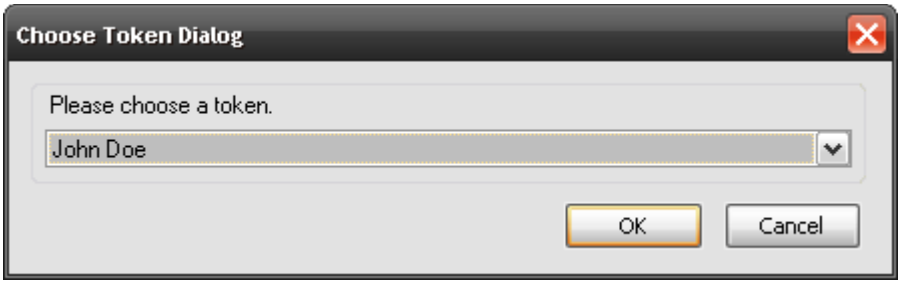
- Now, in the Device Manager window, you can see your smart card



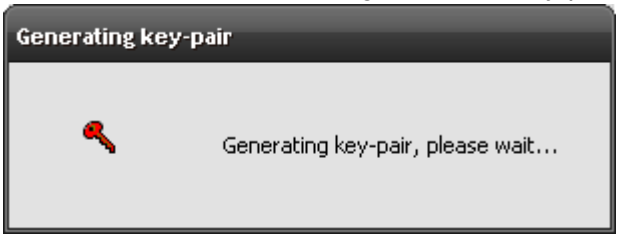
- Click on Log In, then enter your smart card PIN.



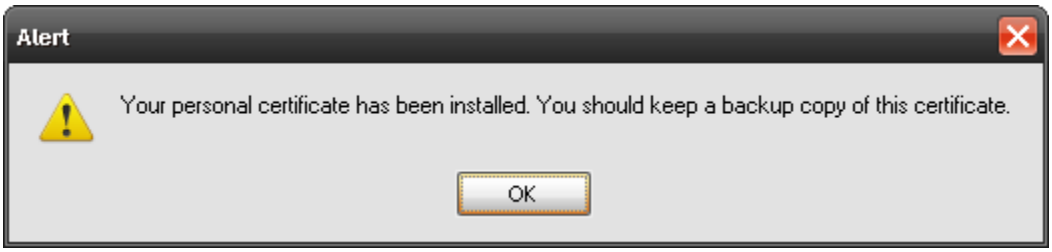
- Next, choose **"Request"** menu, and then click "**Request Certificate**" button
- Enter subject DN, and/or SAN value, choose High Grade, and then click **Generate.** Firefox will ask you to choose your smart card device.



- Click OK, it will take a while to generate the key-pair



- If the certificate is issued immediately, then you click on the Install button in the Certificate Install page.
- If the certificate is issued after approval of your organization registration officer, you must open Firefox in the machine you make the request, view detail of the certificate, and then click on Install. See section 9 to know how to browse and view your certificates. *You might be asked to enter smart card PIN if you had closed the browser after you made the request*
- If the certificate is installed successfully, the message below will be shown.



10 Certificate Management

All of your certificates can be listed and viewed using the Certificate menu. Below is a sample view of the page:

Certificate List

ID	Subject	Effective	Expiration	Serial Number	Status	Display
311	EMail=jdoe@wisekey.com CommonName=John Doe	Sat, 15 Jan 2011 02:23:17 GMT	Sun, 15 Jan 2012 02:23:17 GMT	61E0BB4000000000001F	Active	
310	EMail=jdoe@wisekey.com CommonName=John Doe	Sat, 15 Jan 2011 01:17:33 GMT	Sun, 15 Jan 2012 01:17:33 GMT	61D247AA00000000001E	Active	
309	EMail=jdoe@wisekey.com CommonName=John Doe	Sat, 15 Jan 2011 00:16:45 GMT	Sun, 15 Jan 2012 00:16:45 GMT	619A9D8B00000000001D	Active	

Use the ‘view detail’ button (in the display column) to view the detailed information of a certificate.

Certificate details

Identifying Information

Certificate ID	311
Request ID	359
Status	Active

Details

Issuer	Country=CH Organization=WISeKey OrganizationU
Serial Number	61E0BB4000000000001F
Valid From	Sat, 15 Jan 2011 02:23:17 GMT
Valid Until	Sun, 15 Jan 2012 02:23:17 GMT
Certificate Template	PRA-Advanced

Certificate Subject Information

Identifier		Value
Email	=	jdoe@wisekey.com
Common Name	=	John Doe

Select certificate format to download

Select Format: Base-64 encoded X.509

Select CA Certificate to download

Choose Certificate: WISeKey CertifyID Advanced Services CA 1 Download

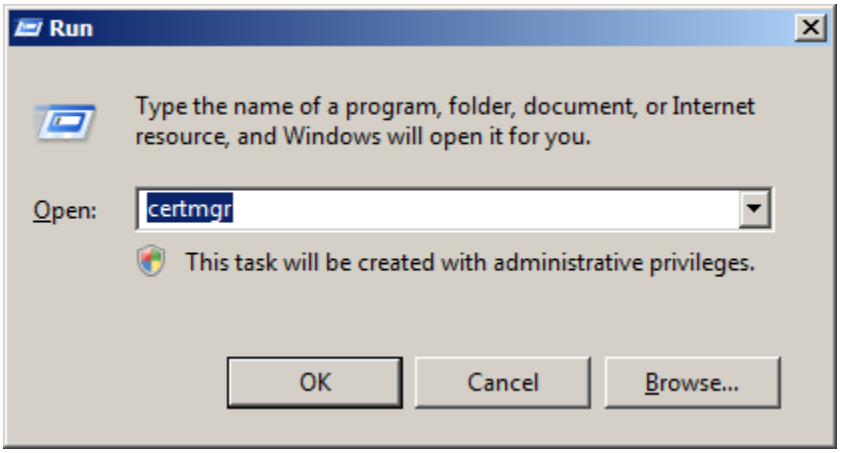
Manage Your Certificate

Download | Renew Certificate | Revoke

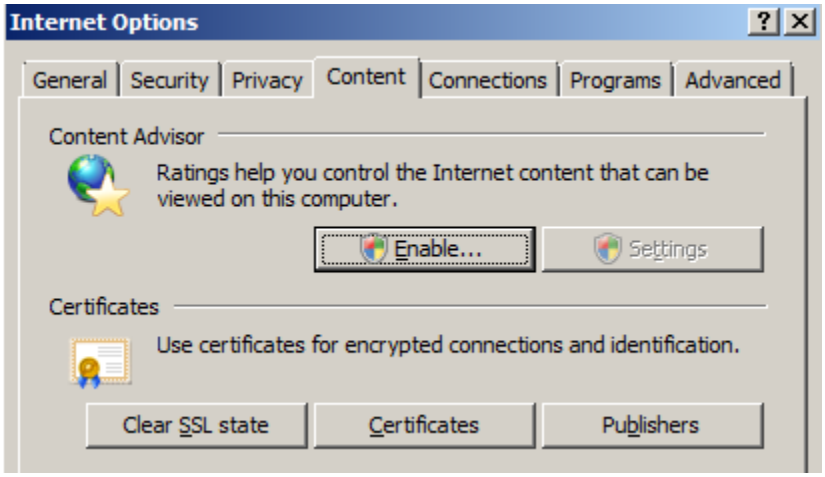
Appendix A: Microsoft Certificate Management

This appendix describes how to open the Certificate Management Program and its certification stores. You can open the Certificate Management Program with the following steps:

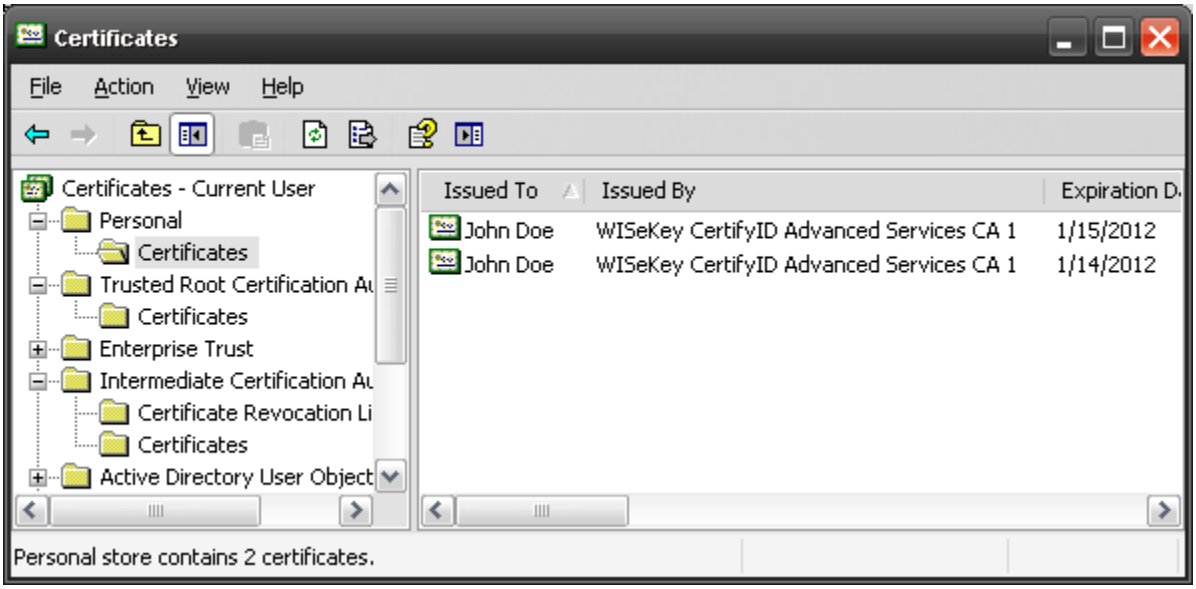
- Run certmgr command from Run window;


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
certmgr
This task will be created with administrative privileges.
OK
Cancel
Browse...

- Click the Certificates button in the Content tab of the Internet Options window



- The Certificate Management Program will appear as shown below:



Where:

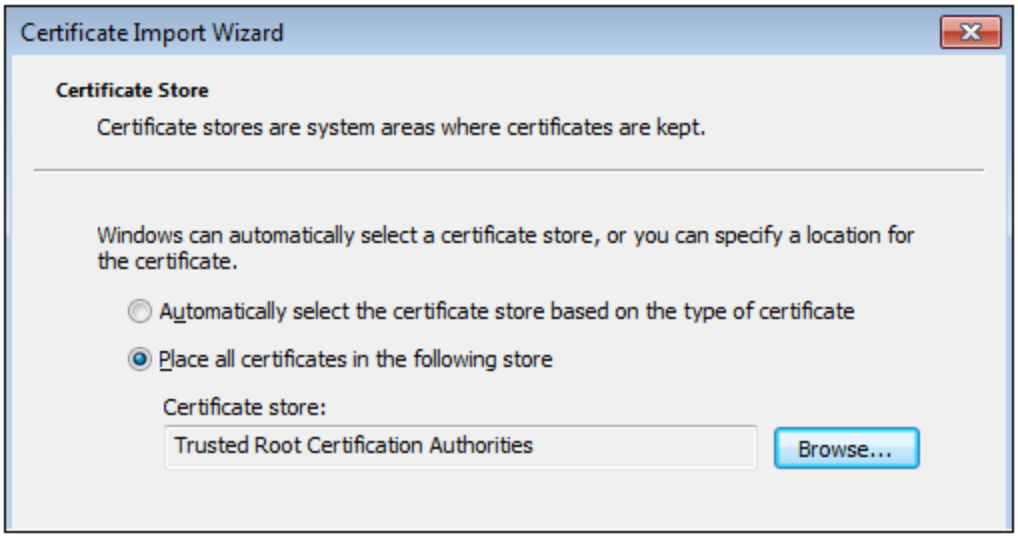
- Personal store contains your certificates
- The Intermediate Certification Authorities (CA store) contains Issuing and Policy certification authorities.
- Trusted Root Certification Authorities (Root store) contains Root Certification Authorities.

How to import a certificate into a certificate store is the same for all certificate stores. Below is an example of how to import WISeKey Root CA Certificate:

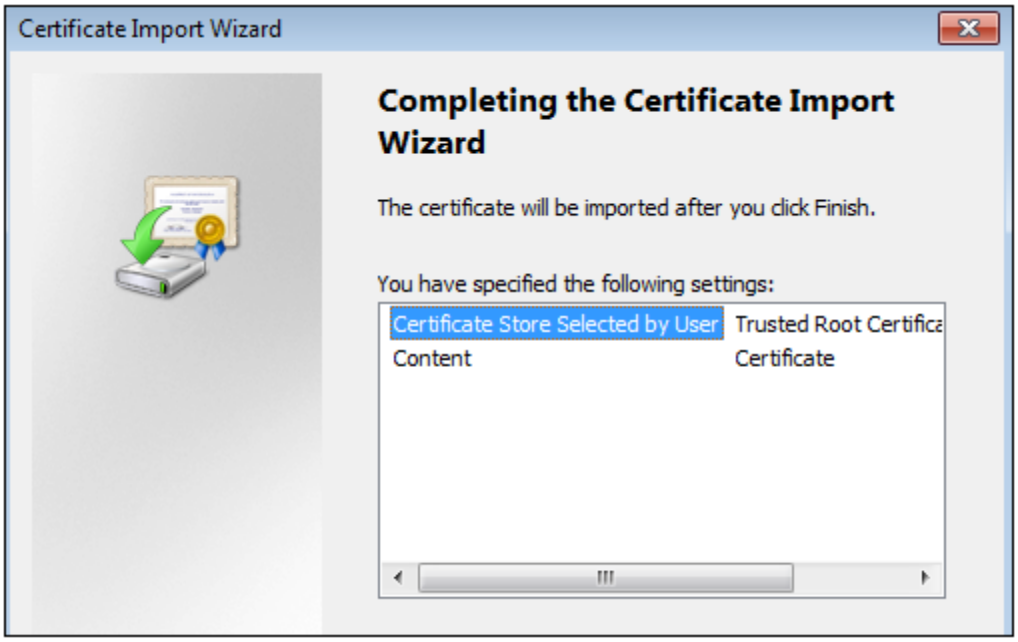
- Check if the certificate to import is available in the certificate store.
- Download Root CA Certificate in Certificate-Install or Certificate-View page. The Root CA certificate is often in the bottom of the CA certificate list.
- Open Trusted Root Certification Authorities store.
- Click Import… button and follow the wizard…

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.

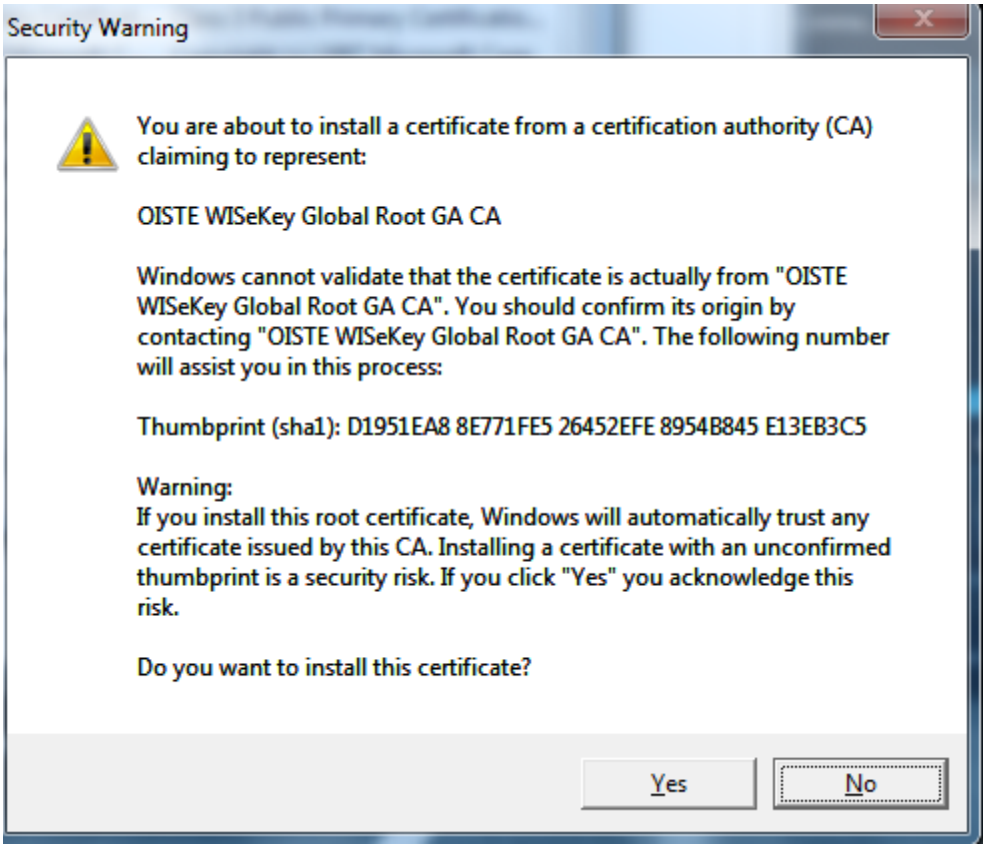
- Browse certificate file…


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities
Browse...

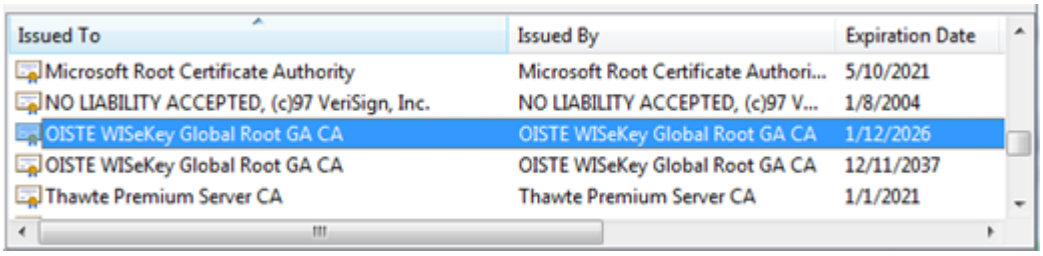
- Next, click Finish


Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User
Trusted Root Certifica
Content
Certificate

- Click Yes


Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
OISTE WISeKey Global Root GA CA
Windows cannot validate that the certificate is actually from "OISTE WISeKey Global Root GA CA". You should confirm its origin by contacting "OISTE WISeKey Global Root GA CA". The following number will assist you in this process:
Thumbprint (sha1): D1951EA8 8E771FE5 26452EFE 8954B845 E13EB3C5
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

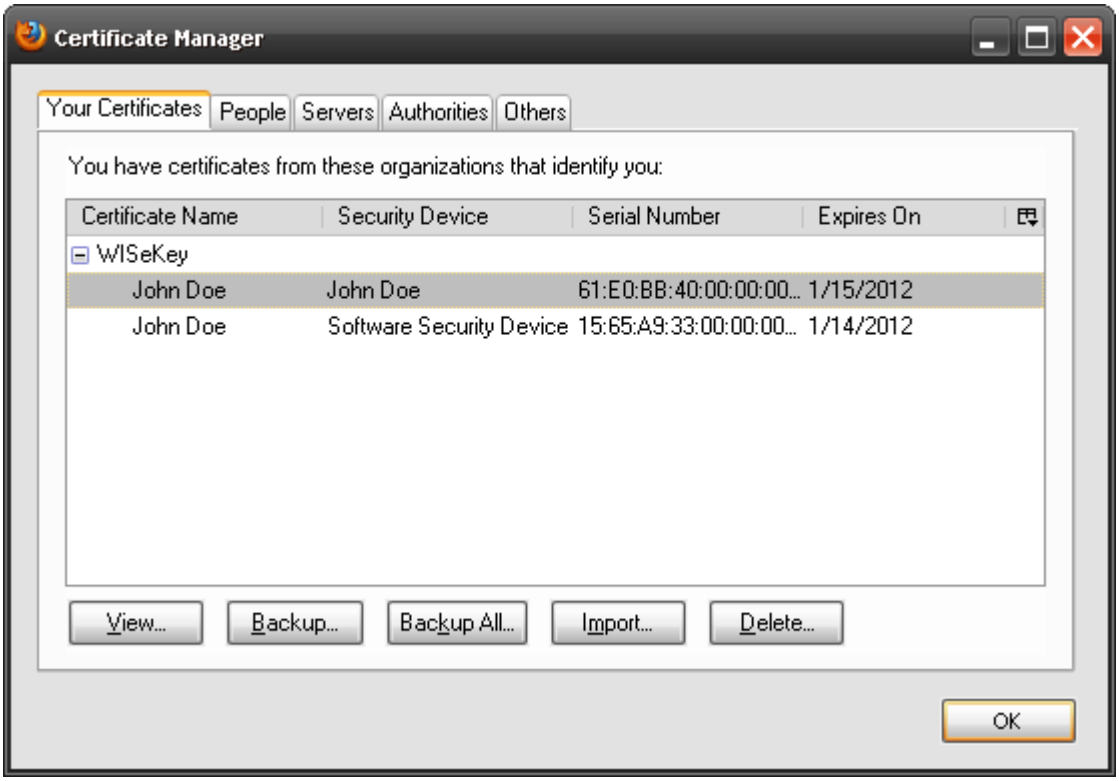
- Now certificate is in the certificate store



Appendix B: Mozilla Firefox Certificate Manager

This appendix describes how to open Firefox Certificate Manager and its certification stores. The program can be opened with the following steps:

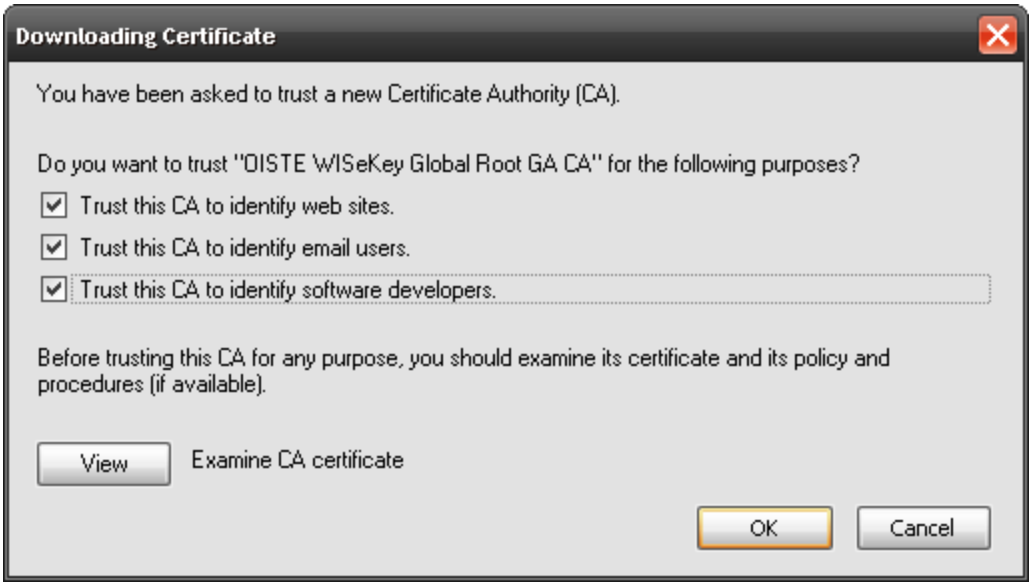
- Open menu Tool/Options…;
- Choose Advanced button in the Options window, choose Encryption tab
- Use “View Certificates” button;
- “Your Certificates” tab lists your entity certificates;



- "Authorities" tab consists of the CA certificates;

How to install a CA certificate is described below:

- Check if the certificate to import is available in the certificate store.
- From the Certificate-Install or Certificate-View page, choose a CA certificate to install, and then select “DER encoded binary X.509” as format to download.
- Click download below the CA certificate list, Firefox will automatically install the certificate after downloading it. A popup window will be shown as follows:


Downloading Certificate
You have been asked to trust a new Certificate Authority (CA).
Do you want to trust "OISTE WISeKey Global Root GA CA" for the following purposes?
Trust this CA to identify web sites.
Trust this CA to identify email users.
Trust this CA to identify software developers.
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).
View
Examine CA certificate
OK
Cancel

- Click OK, and then do the same for the rest CA certificates of the WISeKey including:
  - WISeKey CertifyID Advanced G1 CA;
  - WISeKey CertifyID Advanced Services CA1;